REMARKS

The Office Action mailed September 21, 2007, has been received and the Examiner's comments carefully reviewed. In the present response, claims 1-29 are pending, with claim 9 being amended. No new matter has been added by way of these amendments. Favorable reconsideration of this application is requested in view of the following remarks.

Specification

In the present response, updated priority claim information has been provided, specifically referencing the serial number (60/538,960) of the provisional patent application filed on January 23, 2004, and to which the present application claims priority. Priority was claimed at the time the application was filed; however, no serial number designation had been received by Applicants. Applicants respectfully request that the priority information be noted and entered by the Examiner.

Drawings/Specification

In the Office Action, the drawings filed on January 29, 2004 have been objected to under 37 CFR 1.84(p)(5) because they do not include appropriate reference signs. Applicants respectfully traverse this objection. Applicants note that, due to a typographical error, the internal network denoted with the reference numeral 110 was alternately referenced by the numbers 108 and 110 in the specification. Applicants have amended the single paragraph of the specification using reference numeral 108, and have clarified that those should properly be labeled with reference numeral 110. Applicants assert that this clarification renders the objection to the drawings moot, and respectfully requests reconsideration and withdrawal of this objection.

Claim Rejections - 35 USC §102

In the Office Action, claim 24 has been rejected under 35 U.S.C. §102(e) as being anticipated by Chesla et al. (U.S. Patent Publication No. 2004/0250124). Applicants respectfully traverse this rejection.

Claim 24 as presented herein requires, among other elements, "a database of event records for each message received within a period of time by a computing system and identified as a threat by one or more monitor modules on the computing system." Each of the event records of the claim includes a priority level of the message assigned by one or more of the monitor modules, an event identifier, an event type, an event description, an event priority, a date and time associated with the message, data identifying the message's source, and data identifying the message's destination. Applicants assert that Chesla et al. fails to disclose various elements of this claim.

First, Chesla et al. does not disclose a database of event records as required by claim 24. Chesla et al. discloses a network protection appliance communicatively coupled between a wide area connection and a protected network in order to filter malicious network attacks directed toward the protected network (see, e.g. Chesla et al., Figure 2). The Office Action indicates that the database of event records generally corresponds to some portion of a learning model (Office Action, page 3). However, the database disclosed in the cited portion of Chesla et al. corresponds to only a long-term learning model; that database does not contain any event records as recited by the claims. Rather, average levels of traffic parameters are used. Chesla et al., ¶¶245-248. Chesla et al. therefore does not disclose a database of event records for each message received within a period of time by a computing system and identified as a threat by one or more monitor modules on the computing system.

Second, Chesla et al. does not disclose event records having event data provided by the one or more monitor modules that identified the message as a threat and including the various claimed data elements (event identifier, event type, event description, etc.). The Office Action itself admits at page 9 that "Chesla et al. fails to disclose receiving event data from said modules, [and] storing event data in a database." Furthermore, and with respect to the specific event data claimed, the Office Action selects portions of Chesla et al. that describe disparate aspects of network traffic; not a collection of event data in an event record. For example, the Office Action points to: information about a stateful connection controller as disclosure of event data including priority levels (Office Action, page 4); background information about firewalls as disclosure of monitoring data identifying a message's destination (Office Action, page 5); and still further prior art characterizations as disclosure of data identifying a message's source (Office Action at

pages 5-6). However, the Office Action does not allege (and cannot allege) that these data elements are collected into an event record. Even if Applicants agreed that each of the data elements of claim 24 are in fact described in Chesla et al. (a point which Applicants do not concede), the data elements referenced in the Office Action are disclosed as part of disparate portions of network security systems (e.g. a firewall, a "stateful" controller, and a prior art network appliance, respectively). Notably, none of the cited portions of Chesla et al. collect information into a common event record for storage in a database, or receipt of such data from a monitor module. Therefore, this aspect of claim 24 is not disclosed by Chesla et al as well.

For at least the above reasons, Applicants respectfully assert that Chesla et al. does not anticipate claim 24. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of this claim.

Claim Rejections - 35 USC §103

A. Claims 1-4, 8-9 and 14-15

In the Office Action, claims 1-4, 8-9 and 14-15 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Bhattacharya et al. (U.S. Patent Publication No. 2004/0133672). Applicants respectfully traverse this rejection.

Independent claim 1 requires, among other elements, "storing the event data in a first event record in a database on the computing system, the database including a plurality of second event records containing event data related to previous messages, and analyzing, after receipt of event data from any one of the plurality of monitor modules, the first event record and second event records in the database." Independent claim 9 requires, among other elements, "storing the new event data at the security facility in an event database that includes pre-existing event data," and "calculating, at the security facility and based on the new and pre-existing event data in the event database, a network threat level for the message." Applicants respectfully assert that at least these elements of each of these claims is not taught or suggested by the combination of Chesla et al. and Bhattacharya et al.

Regarding claim 1, Applicants note that the combination of Chesla et al. and Bhattacharya et al. at least fails to disclose storing event data related to the message as an event

record in a database containing second event records containing event data related to previous messages and analyzing the event record and the second event records in the database, as required in claim 1. Applicants note that the Office Action admits at page 9 that "Chesla et al. fails to disclose receiving event data from said modules, [and] storing event data in a database." Applicants assert that Bhattacharya et al. also fails to disclose or suggest such an element. Bhattacharya et al. relates to a network security monitoring system that identifies threats and compares messages with constraints held in a decision graph. Bhattacharya et al., ¶¶0009-0011. "When receiving a new event message, the message is compared with the constraint of a leaf node (of a decision graph)." Id. Constraints in the event graph correspond to inter-event constraints that allow that system to categorize the new event. Conversely, the claimed invention requires analyzing, after receipt of event data from any one of the plurality of monitor modules, the first event record and second event records in the database. Therefore, Bhattacharya et al. also does not teach or suggest this element.

Bhattacharya et al. in fact teaches away from storing past event records in a database for use in analysis, as required by claim 1, in favor of use of the event tree of partial solutions. Bhattacharya et al. indicates that "[a] problem with this [database] methodology is that while it performs well as an offline process, it does not scale well to handle a high volume of incoming events in real time." Bhattacharya et al. therefore cannot be combined with Chesla et al. or another reference to teach storage of event records in a database for analysis of those event records, as claimed.

Regarding claim 9, Applicants note that the combination of Chesla et al. and Bhattacharya et al. at least fails to disclose storing the new event data at the security facility in an event database that includes pre-existing event data, and calculating, at the security facility and based on the new and pre-existing event data in the event database, a network threat level for the message. As described in conjunction with claim 1, the Office Action admits that Chesla et al. does not disclose these elements of the claim. Further, Bhattacharya et al. does not disclose this aspect of claim 9, and cannot be combined with Chesla et al., for at least the same reasons as set forth above for claim 1.

For at least the above reasons, Applicants respectfully assert that claims 1 and 9 are not rendered obvious by the combination of Chesla et al. and Bhattacharya et al. Applicants respectfully request reconsideration and withdrawal of the rejection of these claims.

Regarding the dependent claims, claims 2-4 and claim 8 depend from claim 1, and inherit all of the limitations of that independent claim. Likewise, claims 14-15 depend from claim 9, and inherit all of the limitations of that independent claim. Applicants assert that these claims are not rendered obvious by the combination of Chesla et al. and Bhattacharya et al. for at least the same reasons as described in conjunction with those independent claims. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of these claims as well.

B. Claims 5, 7 and 16

In the Office Action, claims 5, 7 and 16 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Bhattacharya et al. and further in view of Lin et al. (U.S. Patent No. 6,405,250). Applicants respectfully traverse this rejection.

Claims 5 and 7 depend from claim 1, and inherit all of the limitations of that claim. Claim 16 depends from claim 9, and inherits all of the limitations of that claim. Applicants note that the addition of Lin et al. cannot overcome the deficiencies pointed out in part A, above, with respect to the combination of Chesla et al. and Bhattacharya et al., and that the Office Action only applies Lin et al to teach Bayesian probability analysis. Regardless of whether Lin et al. in fact teaches the additional elements recited in claims 5, 7, and 16, (a point which applicants do not concede) the overall combination of references is defective for at least the reasons described above in part A. Therefore, for at least the same reasons as previously recited, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 5, 7, and 16.

C. Claims 6 and 13

In the Office Action, claims 6 and 13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Bhattacharya et al. and in further view of Snapp (U.S. Patent Publication No. 2003/0172064). Applicants respectfully traverse this rejection as well.

Claim 6 depends from claim 1, and inherits all of the limitations of that claim. Claim 13 depends from claim 9, and inherits all of the limitations of that claim. Applicants note that the addition of Snapp cannot overcome the deficiencies pointed out in part A, above, with respect to those independent claims. Again, regardless of whether Snapp teaches "deleting from the event database [pre-existing event data / second event records] that are older than a specified age" (a point on which applicants express no view) the overall combination of references is defective for at least the reasons described above in part A. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claims 6 and 13 for at least the same reasons.

D. Claims 10-11

In the Office Action, claims 10-11 are rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Bhattacharya et al. and in further view of James et al. (U.S. Patent No. 6,993,022). Applicants respectfully traverse the rejection of these claims.

Claims 10-11 depend from independent claim 9, and inherit all of the limitations of that claim. Applicants note that the addition of James et al. cannot overcome the deficiencies pointed out in part A, above, with respect to that claim. Regardless of whether James et al. teaches the additional claim elements recited in claims 10-11, the overall combination of references remains inadequate for at least the reasons described in connection with claim 9 (and claim 1 by reference). Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claims 10-11.

E. Claim 12

In the Office Action. claim 12 is rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Bhattacharya et al. and in further view of Eshghi et al. (U.S. Patent Publication No. 2002/0165954). Applicants respectfully traverse the rejection of these claims.

Claim 12 depends from independent claim 9, and inherits the limitations of that claim. The addition of Eshghi et al. cannot overcome the deficiencies of the combination of Chesla et al. and Bhattacharya et al. pointed out with respect to claim 9, described in part A, above, regardless of whether it discloses "wherein the commands include at least some of the new event data identifying messages for the second computing system to act on and an action to be

performed on the identified messages" (Applicants reserve the right to argue that Eshghi in fact does not disclose this element). For at least the same reasons as set forth with respect to claim 9, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 12.

F. Claims 17 and 21-23

In the Office Action, claims 17 and 21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier et al. (U.S. Patent Publication No. 2002/0087882 A1) in view of Chesla et al. It is assumed that, based on the application of Schneier et al. and Chesla et al. to claims 22-23 that the same combination of references applies to those claims. Office Action at pp. 20-22. Applicants respectfully traverse the rejection of these claims.

Independent claim 17 requires, among other elements, "if the message is identified as a potential threat by one or more of the monitor modules, storing the output of the monitor modules related to the message in a new event record in a database containing a plurality of previous event records, the output including event data describing attributes of the message, a threat type, and an assigned priority; [and] analyzing event records in the database." Applicants assert that at least this aspect of claim 17 is not taught or suggested by the combination of Schneier et al. and Chesla et al.

The combination of Schneier et al. and Chesla et al. fails to teach or suggest "if the message is identified as a potential threat by one or more of the monitor modules, storing the output of the monitor modules related to the message in a new event record in a database containing a plurality of previous event records, the output including event data describing attributes of the message, a threat type, and an assigned priority; [and] analyzing event records in the database." Schneier at least fails to disclose or suggest storing event records in a database which include a threat type. The Office Action acknowledges that Schneier et al "fails to disclose if the message is identified as a potential threat by one or more of the monitor modules." Office Action, p. 18. Schneier et al. logically cannot disclose event data including threat type, because a threat type is determined once a potential threat is identified and categorized.

Schneier et al. also fails to disclose storing the output of the monitor modules related to a potential threat message in a new event record in a database containing a plurality of previous

event records. Schneier et al. only discloses a "variety of knowledge databases containing detailed information helpful for investigating, evaluating, and responding to incidents. Security intelligence databases can contain information about, among other things, the characteristics of various network hardware and software products, known vulnerabilities of such products, the use and characteristics of various hacker tools, and known effective and ineffective responses to various kinds of attacks." Schneier et al., ¶0013. This information is not event record information relating to messages received and identified as potential threats by monitor modules, and as such cannot teach such an element as recited in the claim.

Chesla et al. also fails to disclose a number of the same elements of claim 17. The Office Action admits at page 9, in conjunction with the rejection of claim 24, that "Chesla et al. fails to disclose receiving event data from said modules, [and] storing event data in a database." Further, with respect to claim 17, the Office Action does not allege that Chesla et al. includes storing the output of the monitor modules related to a potential threat message in a new event record in a database containing a plurality of previous event records. Therefore, Chesla et al. cannot teach all of the elements not present in Schneier et al., and the combination of these two references does not render claim 17 obvious.

For at least the above reason, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 17. Similarly, claims 21-23 depend from independent claim 17, and inherit all of the limitations of that independent claim. Applicants therefore assert that each of these claims is not rendered obvious by the combination of Schneier et al. and Chesla et al. for at least the same reasons. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of these claims as well.

G. Claim 18

In the Office Action, claim 18 is rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier et al. (U.S. Patent Publication No. 2002/0087882 A1) in view of Chesla et al. and in further view of Snapp.

Claim 18 depends from claim 17, and inherits all of the limitations of that claim. Applicants note that the addition of Snapp cannot overcome the deficiencies pointed out in part

F, above, with respect to claim 17. Again, regardless of whether Snapp teaches "deleting from the event database previous event records that are older than a specified age" (a point on which applicants express no view) the overall combination of references is defective for at least the reasons described above. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claim 18 for at least the same reasons.

H. Claim 19

In the Office Action, claim 19 is rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier et al. in view of Chesla et al. and in further view of Bhattacharya et al.. Applicants respectfully traverse the rejection.

Claim 19 depends from claim 17, and inherits all of the limitations of that independent claim. Applicants note that the addition of Bhattacharya et al. cannot overcome the deficiencies pointed out in part F, above, with respect to claim 17. Regardless of whether Bhattacharya et al. teaches the added element of claim 19, "wherein the determining operation is repeated each time a new event record is received" (Applicants do not concede this point), the overall combination of references remains defective for at least the reasons previously described. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claim 19.

I. Claim 20

In the Office Action, claim 20 is rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier et al. in view of Chesla et al. and in further view of Bhattacharya et al. and in further view of Lin et al. (U.S. Patent No. 6,405,250). Applicants respectfully traverse the rejection.

Claim 20 depends from claim 17, and inherits all of the limitations of that claim. Applicants note that the addition of Lin et al. cannot overcome the deficiencies pointed out in part F, above, with respect to claim 17. Regardless of whether Lin et al teaches the added elements of claim 20, "identifying all event records in the database that relate to the new event record; performing a Bayesian analysis on the event data in the identified event records; and estimating a threat level for the message based on the results of the Bayesian analysis" (Applicants do not concede this point), the overall combination of references remains defective

for at least the reasons previously described. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claim 20.

J. Claims 25-26 and 27-29

In the Office Action, claims 25-26 are rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Noda et al. (U.S. Patent No. 6,816,890). Additionally, claims 27-29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla et al. in view of Mathews et al. (U.S. Patent Publication No. 2003/0061256). Applicants respectfully traverse these rejections.

All of claims 25-29 depend from independent claim 24, and therefore inherit all of the limitations of that claim. As previously explained, Chesla et al. fails to disclose (1) a database of event records for each message received within a period of time by a computing system and identified as a threat by one or more monitor modules on the computing system, or (2) event records having event data provided by the one or more monitor modules that identified the message as a threat and including the various claimed data elements (event identifier, event type, event description, etc.). Neither the combination of Noda et al. nor Mathews et al. with Chesla et al. teaches or suggests either of these elements. Further, combination of Chesla et al. with either of these references is improper.

1. Claims 25-26

Noda et al. generally describes implementing an L2TP Access Concentrator (LAC) in a gateway apparatus. Noda et al. relates to data routing using L2TP, and does not relate to network security. Noda does not include any monitor modules that identify threats, and does not include a database of event records based on identified threats. Noda et al. therefore does not teach the elements of these claims which are lacking in Chesla, as previously explained with reference to claim 24. Therefore, Noda cannot, in combination with Chesla et al., teach or suggest all of the elements of claims 25-26, in that the combination lacks elements of independent claim 24.

Furthermore, Applicants assert that Noda et al. should not be combined with Chesla et al. The Office Action indicates that "it would be obvious to a person of ordinary skill in the art at the time the invention was made to incorporate an L2TP access concentrator . . .with a database

of records. . .as taught by Chesla et al for the purpose of event routing." Page 33. Applicants disagree with this characterization. Applicants note that the system described in Chesla et al. provides a network security appliance placed between a wide area network and a protected network, and acts as a filter for network traffic entering the protected network. *See* Chesla et al., Figure 2; abstract. The L2TP access concentrator of Noda et al. reviews source and destination addresses, as well as ports, URLs, and whether a message source is local to the LAC to determine whether outbound web requests received from user terminals local to the LAC can be rerouted to a web cache server that is also local to the LAC, thereby minimizing network traffic on the LAC-LNS link and across ISP networks. See Noda et al., Figure 1; col. 17:42-65. Because Chesla et al. provides a preemptive filter for inbound traffic, it would not require the event routing capabilities present in Noda et al. Rather, review and storage of the various information recited in claim 24, particularly whether a message source is internal to the computing system, would be superfluous to the system of Chesla et al., which concerns protection from external (not internal) attacks.

For at least these reasons, Applicants assert that the combination of Chesla et al. and Noda et al. does not render claim 24, and therefore claims 25-26, obvious. Applicants therefore respectfully request reconsideration and withdrawal of the rejection of these claims.

2. Claims 27-29

Mathews et al., in combination with Chesla et al., fails to teach or suggest each of the elements of claim 24, and by implication each of the elements of claims 27-29. Mathews et al. generally describes a transaction processing system used to control transactions relating to information services. Mathews et al. does not relate to network security, and therefore does not include monitor modules that identify threats, and does not include a database of event records based on identified threats. Mathews et al. therefore does not teach the elements of these claims which are lacking in Chesla, as previously explained with reference to claim 24. Therefore, Mathews cannot, in combination with Chesla et al., teach or suggest all of the elements of claims 27-29, in that the combination lacks elements of independent claim 24.

Secondly, Mathews et al. teaches away from combination with Chesla et al in the manner claimed. As quoted on page 34 of the Office Action, Mathews et al. discloses a system "for

allowing such classified services to conduct transactions with other services without explicitly identifying the source or targets of the transaction." Mathews et al. therefore teaches away from the database as described in claim 24 (and upon which claims 27-29 depend) in which an event record is stored that includes, among other data elements, "data identifying the message's source, and data identifying the message's destination."

Finally, and with respect to all of claims 25-29, Applicants note that no view is currently expressed as to whether either Noda et al. or Mathews et al. discloses the specific additional elements recited in dependent claims 25-29; Applicants reserve the right to make additional arguments in the future, as necessary, in support of the patentability of these claims.

Conclusion

It is respectfully submitted that each of the presently pending claims is in condition for allowance and notification to that effect is requested. Although certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentably distinct. Applicants reserve the right to raise these arguments in the future. The Examiner is invited to contact Applicants' representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(612) 332-5300

Dated: March 20, 2008

John C. Reich
Reg. No. 37,703
JReich/AJL/dc